European Research Studies Journal
Volume XXV, Issue 3, 2022

pp. 299-313

Financial Cybercrimes in Poland – In the Search of Victimization Factors

Submitted 01/09/22, 1st revision 21/09/22, 2nd revision 05/10/22, accepted 25/10/22

Jan Garlicki[1], Daniel Mider[2]

Abstract:

Purpose: *Hereby article examines the factors influencing the victimization of adult Poles in the field of financial cybercrimes. Social and demographic factors as well as skills and habits in the field of cybersecurity were taken into account.*

Approach/Methodology/Design: *The method of computer assisted telephone interviews (CATI) was used for this purpose. Descriptive statistics and selected inductive statistics were used in the analyzes. In turn, intra-group differentiation was investigated using a statistical exploratory method called two-step cluster analysis. The analyzes were carried out in the following three groups, those who experienced financial cybercrimes, those who experienced non-financial cybercrimes, and those who did not experience any cybercrime.*

Findings: *The results of foreign studies show contradictions in the answer to the question of what social and behavioral characteristics induce victimization. The use of the cyber-victimized persons segmentation procedure allowed to explain this contradiction, which from now on can be treated as apparent. Among the cyber-victimized group there are several groups that differ in terms of sociodemographic (gender, age, education, income, place of residence) and behavioral (IT competences). These are both groups with low IT competences as well as medium or high. They are both young people and middle-aged and elderly people. An important observation is also that the group structures captured in this way are similar among the victimized and non-victimized, and among the victims of financial cybercrimes and non-financial crimes.*

Practical implications: *Identification of significant features (social, demographic, psychographic and the level of competence in the field of avoiding cyber threats) of people particularly vulnerable to victimization, allows to indicate who can be used awareness-raising, educational and remedial measures. The article addresses the urgent and heavily underinvested need to ensure cybersecurity of ordinary Internet users, especially those who are less able to cope with technical issues, for whom age, disability or other reasons prevent such activity. This is of particular importance in the face of the implementation of further digital services as part of e-government activities.*

Originality/Value: *This is the first study on a nationwide sample of adult Poles that reveals the relationship between cybercriminalization in the field of financial crimes, and socio-psycho-demographic features, as well as IT competences and knowledge of the respondents.*

Keywords: *Financial crimes on the Internet, cybercrimes, cybersecurity, demographic factors, economic factors.*

Paper Type: *Research paper.*

[1] *Tenure professor, University of Warsaw, Poland, e-mail: jgarlicki@uw.edu.pl*

[2] *Adjunct professor, University of Warsaw, Poland, e-mail: d.mider@uw.edu.pl*

1. Introduction

Crime on the Internet is quickly becoming one of the most widespread and costly crimes of the 21st century. In 2019, the losses caused by cybercrime in Poland amount to over a billion dollars (PLN 4.8 billion), and the average cost per victim is USD 142 (PLN 672). There are 7.2 million victims of cybercrime in Poland annually. Globally, 556 million people become victims of cybercriminals each year (Wydział do Walki z Cyberprzestępczością, KWP Kielce). It should be added that the scale of cybercrimes is undoubtedly higher, as numerous victims do not report victimization.

Many people are not even aware that they have fallen victim to a crime or are unable to quantify the losses they have suffered (Button, Lewis, and Tapley, 2009; Cross and Blackshaw, 2014). At the same time, it is a danger that the entities of power cannot cope with on their own, having to resort to support and close cooperation from commercial enterprises (ENISA, 2021). Moreover, the social awareness of cybersecurity of ordinary Internet users (both importance as well as knowledge and skills) is clearly limited. Despite the fact that the issue of cyber threats is recognized as one of the most important challenges facing governments today, education on cybercrime and protection against it has only recently attracted the attention of Polish authorities.

It is also not indifferent that more and more commercial, non-commercial and governmental services are available online (there are over 500 e-government services in Poland), therefore the questions about who (what social groups) and why experience cyber crime, as well as what security measures are used by ordinary people on their computers and smartphones.

The following research questions were posed:

- *Which social groups distinguished on the basis of socio-psycho-demographic criteria are the most susceptible to cyber crime, and which are the least? What socio-demographic categories (gender, age, education, material status, size of the place of residence, occupation) are important in this respect?*
- *What types of attitudes (understood as knowledge, skills and practices in the field of online security) towards cyber threats can we distinguish in Polish society and how numerous are they?*
- *Are there sociodemographic differences between vulnerable financial types and other non-financial types of crime (insults and defamation, intimidation, loss or disclosure of private data, relationship fraud)?*
- *Is the level of awareness of cyber threats related to the experienced victimization in this area and how?*
- *Do the knowledge, skills and actions taken in the face of cyber threats influence the level of fear towards them?*

The victims of cybercriminals suffer numerous damages: material, moral and image-related losses, emotional trauma related to the experience of a crime and trauma related to criminal proceedings against the perpetrator of the crime, fear of using the Internet, in particular financial services, arise. In the long run, this phenomenon leads to a diversification of life chances and even the standard of living. Knowledge of particularly vulnerable social groups is important both from the point of view of individuals and internal security.

The article responds to the urgent and heavily underinvested need to ensure Internet security for ordinary Internet users, especially those who are less able to cope with technical issues, for whom they prevent such activity due to their age, disability or other reasons. This is of particular importance in the face of the implementation of further digital services as part of e-government activities.

An important premise for undertaking this research topic is the fact that empirical research on cyber crime on representative national samples for a given country is relatively rarely conducted (van Wilsem, 2013; Reyns and Henson, 2016; Holt, Burruss, and Bossler, 2018; Reep-van den Bergh and Junger, 2018; Virtanen, 2017), moreover, these results often differ and are contradictory (Reep-van den Bergh, Junger, 2018).

2. Materials and Methods

The answers to the research questions were determined in the course of a quantitative empirical study conducted by the Association of Political Science Graduates (Stowarzyszenie Absolwentów Nauk Politycznych) affiliated with the Faculty of Political Science and International Studies at the University of Warsaw.

The research was financed by the Justice Fund (Fundusz Sprawiedliwości) administered by the Minister of Justice. The survey entitled *Cybersecurity – awareness, fear, counteraction* was conducted from 12 to 30 June 2021 using computer-assisted telephone interviews on a representative (sex, age, place of residence and education) sample of N=1,000 adults (18+) of Poles. The results of the measurement, exhausting the requirements of the so-called statistical representativeness, can be generalized from the sample to the population of adult Poles.

The technique of computer-assisted telephone interviews was preferred over classic standardized face-to-face interviews (Face to Face, F2F, Paper and Pencil Interviews, PAPI) and online surveys (Computer Assisted Web Interviews, CAWI. Compared to these techniques, CATI interviews have a number of methodological, psychological-interactive and organizational-technical advantages that make them particularly useful in this research project.

The selection of the sample is statistically representative and was carried out using a method called Random Digit Dialing (RDD) (Mitofsky, 1970; Wakesberg, 1978). This method is considered by researchers as optimal and classic (Potthoff, 1987). It is constantly modernized in research practice (Tucker *et al.*, 1992), and new phenomena such as the impact of the development of mobile telephony are also taken into account (Brick *et al.*, 2007; Keeter *et al.*, 2008). This method allows for the random selection of the sampling frame and, as a result, obtaining representativeness in terms of socio-demographic features key for research purposes.

In Western European literature, the concept of Information Security Awareness (ISA) is used to research cyberthreat awareness (Ryan, 2006). The measurement is carried out using the Human Aspects of Information Security Questionnaire (HAIS-Q). It is the globally best known and most widely used quantitative research tool for the holistic measurement of information security awareness.

The research instrument is made up of a battery of 63 indicators grouped into seven thematic areas: password management, email use, internet use, social media use, mobile phone use, information management and incident reporting. Each of the areas was divided into three aspects: knowledge (knowledge of threats and the ability to deal with them), attitudes (attitude towards security practices) and behavior (actual implementation) (Parsons *et al.*, 2017; Cindana and Ruldeviyani, 2018/19). However, this tool has limited applications, as it is mainly used to research security awareness in institutions where the security protocol is established and the users are trained (Bulgurcu, Cavusoglu, and Benbasat, 2010; Taneja, 2007).

The respondents were asked about the experience of cybercrime according to the typology shown in Table 1. Similar, although not identical, categorizations are present in the world literature on the subject (Button, McNaughton, Kerr, Owen, 2014; and Chang 2008, Cross, Smith, and Richards, 2014).

Table 1. *Typology of cybercrimes divided into financial and non-financial.*

Typology of cybercrimes	
Fraud on an auction or other website (Allegro, Olx, Sprzedaż-my, Lento, Amazon)	**Financial cybercrimes**
Scam in the online store	
Fraud or attempted financial fraud by email, instant messaging or social media account	
Financial loss due to an attack on online bank account (or other financial service)	
Cryptocurrency fraud	
Dating site fraud - the financial type	
Insulting in internet conversations	**Non-financial cybercrimes**
Unwanted (individual or group) messages sent for the purpose of bullying or intimidation	
Human relationship fraud (including attempted fraud) by email, messaging, or social media account	

Data loss or theft / disclosure as a result of an attack on an e-mail account	
Data loss or theft / disclosure due to an attack on a social media account (Facebook, Twitter, LinkedIn, etc.) and account hijacking	
Dating site scam – human relationship	
Sexual harassment over the Internet	

Source: *Own study.*

For the purposes of comparative analyzes, the following three groups of respondents were distinguished: those who experienced financial cybercrimes, those who experienced non-financial cybercrimes, and those who did not experience any cybercrime but use the Internet. In order to test the homogeneity of each group, segmentation was also made.

For segmentation, a two-stage cluster analysis was used. This particular analytical technique has particularly useful features: the ability to construct a model using both interval and nominal variables, and it allows the analysis of databases with large numbers of units of analysis.

3. Results

One in three Poles who use the Internet (36.5%) has been a victim of cybercrime at least once in their lives. The percentage of multiple victims of cybercrimes is 17.04%. Two-thirds of respondents (63.5%) have never experienced any type of cybercrime in their lives. Three groups are characterized below in turn: those who have experienced financial cybercrimes, those who have experienced non-financial cybercrimes, and those who have not experienced cybercrimes at all.

3.1 Cyber-Victims in the Financial Sphere

In this group, we mainly observe men (54.5% of them, while the total population is 48.4%). They are usually residents of the largest cities (over 500,000 inhabitants), there is a clear predominance of people from the Mazowieckie voivodship. These are usually married people who describe their financial situation as moderately satisfactory.

People with secondary education dominate, they are usually people who have children. In this group, we see a clear advantage of the simplest ways to ensure cybersecurity, such as: not opening suspicious websites, not opening attachments to emails from unknown people, using paid antivirus software, making sure that no one can see the computer screen.

In addition, 36.4% of the surveyed people in this group do not work under an account with administrator privileges, and moreover, these people use password managers and encryption slightly more than others. It should be noted that the passwords created in this group are slightly longer (they also change them slightly more often than the general ones) than the passwords of all respondents, but insufficient from the point of view of security.

They are also people who use the Internet slightly more than the general public, the average here is just over 9 hours a week using the telephone and 14 hours using the computer, while for the general public it is about 7 hours using the telephone and approximately 14 hours using the computer. The observed results are inconsistent and inconsistent, the group is diverse. Only the separation of two groups using the cluster analysis technique eliminates this incoherence and reveals two groups with significantly different competences in terms of the level of awareness of threats and the ability to prevent them.

Segment A. There is a significant advantage of women in relation to the total number of women (56.7%, while among the general population – 45.5%). The first group includes mainly people aged 18 to 24, 25 to 44 and over 65. They are mainly villagers. We notice an overrepresentation of people from the Małopolskie, Dolnośląskie, Śląskie, Lubuskie and Podkarpackie voivodeships. These people slightly more often report moderate financial problems (item: "we live very frugally to save for more serious purchases" and "money is enough only for basic needs").

Their net household income ranges between PLN 3,000 and PLN 5,000. People with secondary, vocational and lower education dominate. More often than in other groups, they are single people or living in small two-person households. This group consists of people with low IT competences that do not allow them to cope with even typical threats. However, they are people with a low level of anxiety about cybercrime, despite – or perhaps because of – their limited knowledge and skills.

Segment B. The dominant in this group are men (61.2%). Local age maxima fall in the age categories 35-64 years. They are usually people living in cities with more than 500,000 inhabitants or between 100,000 and 500,000 inhabitants. The inhabitants of the following voivodships are dominant: Wielkopolskie, Mazowieckie and Zachodniopomorskie.

Among the professions performed, we notice an overrepresentation of specialists, as well as office workers and representatives of public authorities, senior officials and managers. These are people who find their household income satisfactory. People with graduate and undergraduate education dominate. These are people who implement slightly more advanced means of protection on the Internet. Every third person in this group (28.9%) uses a VPN.

These are users with a proactive approach to cybersecurity: they learn on their own and read about Internet security (as much as 78.9%). These are people who have a slightly higher level of anxiety and, at the same time, higher confidence in their knowledge of safe use of the Internet**.**

3.2 Victims of Non-Financial Cybercrimes

Age and gender are not a significant differentiating variable in this group. We see small local maxima among people living in cities with 20,000 to 50,000 inhabitants, and 100,000 to 500,000 inhabitants. A characteristic feature in this group is the strong overrepresentation of people with higher education (43.4%), higher engineering education (7.1%) and higher education undergraduate (7.1%). These are people with ambiguous attitudes expressed by knowledge and action against cyber threats. Segmentation was also performed in this group; the algorithm distinguished two groups described below.

Segment C. This group is dominated by the representatives of the young generation aged 18-24 and 25-34. They are mainly villagers. This group is overrepresented as employees of personal services and salespeople. They are relatively low-income people who live frugally. A large group among them are married and married (60.5%) as well as single men and women (23.3%). People with vocational (20.9%) and secondary (27.9%) education dominate.

Every tenth of these people disregard cybersecurity and do not use any (11.6%), while as many as 20.9% use the help of better acquainted family members or friends in this area. If they implement cyber security themselves, it's only the simplest. They are active internet users. On average, they use the Internet for 10 hours (smartphones) and 18.2 hours (computers) per week.

Segment D. Age significantly distinguishes members of this group from the rest of the population. We record local highs among people aged 35-44 and 45-54. Members of this group live in cities with more than 500,000 inhabitants. Representatives of public authorities, officials and managers, and office workers are overrepresented. They are well-off people, their financial situation is expressed by the statement: “it is enough for everything and we still save for the future” (48.6% in this group, and 37.2% in the population).

In this group, as many as 48.6% of respondents have higher education. These are people who usually have children (nearly half of them). They take cyber threats seriously and take a wide range of cyber self-defense measures. These are people active on the Internet. Using a smartphone, they use the Internet (average) 10.5 hours a week, and using computers 17.8 hours a week.

3.3 Non-Cyber-Victimized

These are people who – for various reasons – among people who have never experienced cybercrime. Their social and demographic characteristics are as follows. Gender does not distinguish this group – the distribution is the same as for the entire population. These people do not stand out with anything special in terms of age categories, except for a slight overrepresentation of people aged over 65 and 55-64.

We also see a slight advantage of the inhabitants of villages and cities below 20,000 residents. Within the occupational categories, we see an overrepresentation of people who perform manual work as well as retirees and pensioners. These are people expressing moderate satisfaction with their financial situation, defined by the phrase: "we live sparingly and therefore money is enough".

Net income of between PLN 2,000 and PLN 3,000 and PLN 1,500-2,000 prevail. In terms of marital status, the local maximum is among widowers and widows. People with vocational education predominate, but we also deal here with a large group of people with higher education, master's degree, numbering 22.0 percent. In this group, every fifth person does not use any security measures on the Internet, and also every fifth person implements a security model based on delegating the use of security measures to familiar family members and friends.

The average computer use of the Internet is 12 hours a week, and the average of using the Internet by means of a 5.3 phone is significantly lower than in the other groups. However, the above characteristics are misleading. However, this is the group most diversified among the other groups distinguished. Among people who did not experience cyber crime, the segmentation made it possible to distinguish three different, but almost equal segments:

- Segment E – 29.9%,
- Segment F – 35.7%,
- Segment G – 34.4%.

Segment E. This group is overrepresented between the ages of 25 and 44. They are inhabitants of villages located just outside the city limits. This group is highly diversified professionally – there are both farmers, gardeners, foresters, fishermen, but also personal service workers, sellers, office workers, associate professionals and specialists, as well as representatives of public authorities.

These people are moderately satisfied with their financial status. Quite a large group are unmarried or in cohabitation. Education does not significantly differentiate this group from the average for the entire population. These are people who independently implement cybersecurity solutions, both basic and intermediate. The average weekly Internet use with a smartphone in this group is 6.69 hours, while with a computer it is 13.9 hours.

Segment F. This group is characterized by a clear overrepresentation of women - 61.1%, while for the entire population it is 54.3. These are people aged over 65 (more than half in this group) and aged 55-64 (one fifth in this group). We note here – obviously – an overrepresentation of old age and disability pensioners (65.6%). They are people with various incomes, although we note a small proportion of people who live very frugally to save for more serious purchases. They are usually single people, 24.4% of them are widowers or widows.

Most of these people (59.7%) use the help of family members or friends to implement Internet safety rules. Typically, people who belong to this group do not implement any security measures on their own; they do not know both simple and advanced security.

Their level of fear of cyber threats is at the level of the whole population, while the declarations of the level of knowledge and ability to use the Internet safely are assessed much more pessimistic than the average for the entire population and worse than in other groups. It is worth emphasizing that these are people who, however, use the Internet, although they do it to the smallest extent among other groups, the time spent during the week using the Internet via a smartphone is 5.6 hours and using a computer 8.4 hours.

Segment G. In the third, never cyber-victimized group, we observe male overrepresentation. They are middle-aged people – 35-44 and 45-54 years old. They are usually residents of cities with more than 500,000 inhabitants and towns with up to 100,000 inhabitants, living in the Mazowieckie and Zachodniopomorskie voivodships. In terms of professional roles, we notice a clear overrepresentation of people performing office work, both in managerial positions and regular employees.

These are people who consider their financial situation to be good or very good (as many as 47.40% of them declare net earnings of PLN 5,000 and more). Among them, as much as 58.7% have higher education.

Those belonging to this group implement cybersecurity rules to the highest degree, including: they update system software, have anti-virus programs, use safe operating systems, do not store sensitive documents on external servers, including e-mail servers. These people are mostly proactive towards cybersecurity. Three out of four people in this group (77.02%) independently acquire knowledge about cybersecurity on the Internet, while every fourth (24.8%) participated in cybersecurity courses.

Every fifth of this group (19.2%) uses virtualization to increase their security. Those classified in this group treat the issues of physical security very rigorously, i.e. they do not leave the computer or phone unattended (as much as 89.2% do), and they do not allow any devices to be connected to the phone by other people.

One in six of them (18.3%) implements encryption of the entire hard disk, and one in five (20.7%) uses a software or hardware password manager.

The level of concern about cyber threats in these people is slightly higher than in the rest of the population. They are more aware of cyber threats. It is the most active group in terms of time spent on the Internet. The average of internet use with a smartphone is 8.37 hours and with a computer 19.42 hours per week.

Table 2. *Socio-demographic features of cyber-victimized and non-cyber-victimized people - segmentation using the cluster analysis method.*

Victims of financial cybercrimes		**Victims of non-financial cybercrimes**		**People who have never been a victim of cybercrime**			**Not using the Internet**
24,2%		11,3%		61,9%			2,6%
Segment A	Segment B	Segment C	Segment D	Segment E	Segment F	Segment G	-
9,0%	15,2%	4,3%	7,0%	18,4%	22,2%	21,3%	
Mainly women, 18-24, 25-44 and 65+, moderate or low income, vocational and secondary education	Men, 35-64, inhabitants of cities over 100,000 and over 500,000 residents, specialists, office workers, higher education	18-24 and 25-34, living in villages, low income, secondary education	35-44, 45-54, residents of cities with more than 500,000 and cities of 20-50 thousand, high income, higher education, have children	25-34, 35-44, villages near cities, office workers, specialists, clerks, moderate income, unmarried or cohabiting	Women, 65+ and 55-64, inhabitants of rural areas and the city below 20,000. residents, retirees and pensioners	Men, 35-44 and 45-54, cities over 100,000 and over 500,000 residents, specialists, representatives of public authorities, office workers, high income, higher education	
low level of competence in avoiding cyber threats	medium or high competences	low competences	medium or high competences	medium competences	low competences	medium or high competences	-

Source: *Own study.*

4. Discussion and Conclusion

Research on the victimization of financial-related cybercrimes commonly shows a correlation between victimization vulnerability and such sociodemographic characteristics as gender, age, education and marital status (Titus and Gover, 2001; Whitty, 2017), analogically to classic works on victimization of financial crimes (Lee and Soberon-Ferrer, 1997). However, these dependencies are not clear cut. For example, some researchers consider one of the genders to be more at risk: women (Henry and Powell, 2018) or men (Milani, Caneppele, and Burkhardt, 2020; Sudzina and Pavlicek, 2022). In Poland, women are particularly vulnerable to financial crimes. This applies to the groups of the youngest women (18-24 years old) and seniors (65 and more years old). Gender, on the other hand, turns out to be a negligible factor when dealing with non-financial cybercrimes. This seems to be confirmed – inconclusive – by the results of foreign research in this area.

It is also an abuse to say that cyber crime is positively correlated with the age of the victim. Some results seem to confirm this hypothesis, while others indicate that the most victimized group (however, this applies to all crimes, not only financial crimes) are young people starting the third decade of their lives (Reyns, Fisher, Bosler, and Holt, 2019; Jorna, 2016).

The relationship between education and cyber crime is also ambiguous. Some researchers have shown that victimization negatively correlates with acquired education (Reyns, Fisher, Bossler, and Holt, 2019; Milani, Caneppele, and Burkhardt, 2020), similarly to classic studies (Lee and Soberon-Ferrer, 1997). In turn, Titus and Gover (2001) found that better educated people were more likely to fall victim to fraud. The conducted research has shown that age is a significant correlate of cyber crime, however, of different kinds. Financial cybercrimes are more often exposed to less educated people, and to non-financial crimes people with higher education, but also with secondary education.

The research results and the link between material status and cyber crime are much more ambiguous. Ross and Smith (2011) showed that low-income people are susceptible to financial cybercrimes, middle-earners (in the study of the authors indicated: $ 20-40 thousand) were more likely to fall victim to non-financial fraud, while the probability of cyber crime victimization of high-earners (over $ 40,000) was the lowest compared to other income groups.

Victimization to financial crimes and crimes in general is also explained by behavioral and personality factors (The Big Five Inventory – 2, BFI-2). The aspect of behavior leading to increased susceptibility to victimization is considered within three classical theoretical perspectives: the theory of self-control (Gottfredson and Hirschi, 1990), the theory of routine activity (Cohen and Felson, 1979) and the theory of exposure to lifestyle (Hindelang, Gottfredson, and Garofalo, 1978). This led to one of the most systematic and unsurprising discoveries that more time on the Internet contributes to greater exposure to potential criminals and to victimization (Leukfeldt and Yar, 2016).

The exposure effect was also confirmed in the conducted research: there is a moderate positive correlation between victimization (both financial and non-financial cybercrimes) and the intensity of Internet use. Among the behavioral factors, the relationship between IT competences and victimization was also investigated, but showed no statistically significant relationships (Milani, Caneppele, and Burkhardt, 2020; Kaakinen *et al.*, 2021; Bossler and Holt, 2009).

Similar results were obtained in the study – among cyber-victimized persons there are people with low, medium and high competences in proportions as for the entire population.

The research conducted on the Polish population also confirmed this result. In the literature, traumatic life experiences (e.g., loss of a loved one, accident and health detriment) are indicated as a predictor of cyber crime. Negative life experiences can influence a person's likelihood of becoming a victim of crime. Trauma has a negative impact on the cognitive competences of the respondents, which disturbs judgment, making them more susceptible to further traumas (Chang and Chong 2010; Ross and Smith 2011; Shadel, Pak and Sauer, 2014; Anderson, 2013). The conducted research on the nationwide sample did not address these issues.

The ambiguity of the results in own and foreign research can be explained. The conducted segmentation shows that among cyber crime victims there are several groups with different sociodemographic, psychographic and behavioral characteristics. These are both groups with low IT competences (Segments A and C) and medium or high (Segments B and D). They are both young people (Segment C) and middle-aged and elderly people (Segment B).

An important observation is also that group structures are similar among the victimized and the non-micitimized; in other words, sociodemographic and behavioral characteristics do not differentiate between those who have been victims of cybercrime and those who have not.

Basically, we can distinguish two groups vulnerable to cybercrime acts, whether they are financial cybercrimes or non-financial cybercrimes. The key risk factors identified in the course of own research include: low level of cybersecurity competences in the first group and the intensity of Internet use in the second group, not knowing advanced security measures.

It is true that cybersecurity competences in the second indicated group are generally higher, there is a noticeable more extensive, higher awareness and knowledge, and as a result, the basic security techniques are effectively implemented by this group. Unfortunately, the level of cyber security and awareness remains insufficient.

The majority of this group are people who use the Internet extensively in their professional and private lives. This group is generally much larger among those who have experienced both financial cybercrimes and non-financial cybercrimes. Users included in the first group use the Internet occasionally. Internet access for services and information usually takes place when access to them is not possible by other means. The groups exposed to financial cybercrimes and non-financial cybercrimes are basically the same.

Therefore, we should look for factors other than sociodemographic. It is possible that this issue may be explained by psychographic or lifestyle-related variables.

Knowledge, skills and actions taken in the face of cyber threats are a weak negative correlate of cybercrime fear. Negative experiences in the field of cyber crime do not correlate with the experience of victimization in this area, measured by the number and quality of security measures taken.

The conducted study reveals the structures of cyber victimized people. It therefore offers opportunities that policy makers, the police, third sector organizations and financial institutions can use to improve security and raise awareness of avoiding cyber threats to ordinary Internet users. Identifying groups that differ in terms of different socio-demographic and awareness features allows for the development of educational programs and social campaigns perceptually adapted to people exposed to cyber crime.

References:

Anderson, K. 2013. Consumer fraud in the United States. The third FTC survey. https://www.ftc.gov/reports/consumer-fraud-united-states-2011-third-ftc-survey.

Bossler, A.M., Holt, T.J. 2009. On-line activities, guardianship and malware infection: An examination of Routine Activities Theory. International Journal of Cyber Criminology, 3(1), 400-420.

Brick, J.M., Brick, P.D., Dipko, S., Presser, S., Tucker, C., Yuan, Y. 2007. Cell phone survey feasibility in the U.S.: Sampling and calling cell numbers versus landline numbers. Public Opinion Quarterly, 71, 23-39.

Bulgurcu, B., Cavusoglu, H., Benbasat, I. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34, 523-548.

Button, M., McNaughton, C., Kerr J., Owen, R. 2014. Online frauds: Learnings from victims why they fall for these scams. Australian & New Zealand Journal of Criminology 47(3), 391-408.

Button, M., Lewis, C., Tapley, J. 2009. Fraud typologies and victims of fraud: Literature review. Office of Fair Trading and National Fraud Authority, London.

Chang, J. 2008. An analysis of advance fee fraud on the internet. Journal of Financial Crime 15(1), 71-81.

Chang, J., Chong, M. 2010. Psychological influences in e-mail fraud. Journal of Financial Crime, 17(3), 337-350.

Cindana, A., Ruldeviyani, Y. 2018/19. Measuring information security awareness on employee using HAIS-Q: Case study at XYZ firm. International Conference on Advanced Computer Science and Information Systems, ICACSIS.

Cohen, L.E., Felson, E. 1979. Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588-608.

Cross, C., Smith R.G., Richards, K. 2014. Challenges of responding to online fraud victimisation in Australia. Trends & issues in crime and criminal justice, no. 474. https://aic.gov.au/publications/tandi/tandi474.

Cross, C., Blackshaw, D. 2014. Improving the police response to online fraud. Policing, 1-10.

Emami, C., Smith, R., Jorna, P. 2019. Online fraud victimisation in Australia: Risks and protective factors. Research Report.

Etaki, A., Seidzadeh, S.M., Bashi, M.M. 2021. Risk factors for being a victim of Cyber Theft and Cyber Fraud crimes. Journal of University Studies for inclusive Research, 2(12).

European Union Agency for Cybersecurity (ENISA). 2021. e-Governance Academy (EGA), Raising Awareness of Cybersecurity. https://ega.ee/publication/cybersecurity-awareness/.

Gottfredson, M.R., Hirschi, T. 1990. A general theory of crime. California, Stanford University Press.

Henry, N., Powell, A. 2018. Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19(2), 195-208.

Hindelang, M., Gottfredson, M., Garofalo J. 1978. Victims of personal crime: An empirical foundation for a theory of personal victimization. Ballinger Publishing Company, Massachusetts.

Holt, T.J., Burruss, G.W., Bossler, A.M. 2018. Assessing the macro-level correlates of malware infections using a routine activities framework. International Journal of Offender Therapy and Comparative Criminology, 62(6), 1720-1741.

Jorna, P. 2016. The relationship between age and consumer fraud victimisation. Trends & issues in crime and criminal justice, 519.

Kaakinen, M., Koivula, A., Savolainen, I., Sirola, A., Mikkola, M., Zych, I., Paek, H.J., Oksanen, A. 2021. Online dating applications and risk of youth victimization: A lifestyle exposure perspective. Aggressive Behavior (Advance online publication).

Keeter, S., Dimock, M., Kennedy, C., Best, J., Horrigan, J. 2008. Costs and benefits of full dual frame telephone survey designs. Paper presented at the 63rd Annual Conference of the American Association for Public Opinion Research, New Orlean.

Lee, J., Soberon-Ferrer, H. 1997. Consumer vulnerability to fraud: Influencing factors. Journal of Consumer Affairs, 31(1), 70-89.

Leukfeldt, E.R., Yar, M. 2016. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280.

Milani, R., Caneppele, S., Burkhardt, C. 2020. Exposure to cyber victimization: Results from a Swiss survey. Deviant Behavior, 1-13.

Mitofsky, W. 1970. Sampling of telephone household, unpublished. Central Bureau of Statistics Memorandum.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computer & Security, 66. DOI: 10.1016/j.cose.2017.01.004.

Potthoff, R.F. 1987. Some generalisation of the Mitofsky-Waksberg technique for Random Digit Dialling. Journal of the American Statistical Association, 82, 409-418.

Reep-van den Bergh, C.M.M., Junger, M. 2018. Victims of cybercrime in Europe: A review of victim surveys. Crime Science, 7(1), 5.

Reyns, B.W., Henson, B. 2016. The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. International Journal of Offender Therapy and Comparative Criminology, 60(10), 1119-1139.

Reyns, B.W., Fisher, B.S., Bossler, A.M., Holt, T.J. 2019. Opportunity and self-control: Do they predict multiple forms of online victimization? American Journal of Criminal Justice, 44(1), 63-82.

Ross, S., Smith R.G. 2011. Risk factors for advance fee fraud victimisation. Trends & issues in crime and criminal justice, 420.

Ryan, J.E. 2006. A comparison of information security trends between formal and informal environments. Doctoral Dissertation, Auburn University, Publication No. AAT 3225287.

Shadel, D., Pak, K., Sauer, J, 2014. Caught in the scammer's net: Risk factors that may lead to becoming an internet fraud victim, Washington.

Sudzina, F., Pavlicek, A. 2022. Virtual Offenses: Role of Demographic Factors and Personality Trait, Information, 11, 188. doi:10.3390/info11040188.

Taneja, A. 2007. Determinants of Adverse Usage of Information Systems Assets: A Study of Antecedents of IS Exploit in Organizations. Doctoral Dissertation, University of Texas at Arlington.

Titus, R.M., Gover, A.R. 2001. Personal fraud: The victims and the scams. Crime Prevention Studies, 12, 133-151.

Van Wilsem, J. 2013. Hacking and harassment – Do they have something in common? comparing risk factors for online victimization. Journal of Contemporary Criminal Justice, 29(4), 437-453.

Virtanen, S.M. 2017. Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. Psychiatry, Psychology and Law, 24(3), 323-338.

Whitty, M. 2017. Do you love me? Psychological characteristics of romance scam victims. Cyberpsychology, Behavior and Social Networking, 21(2), 105-109.

Wydział do Walki z Cyberprzestępczością, KWP Kielce.